The Smart Home Network, Attack Vectors and Mitigation

Chijioke Franklin Emejuru

Executive Summary - This assessment focuses on the network setup and penetration testing of a LAN smart home network. The scope of the assessment included analysing the security posture of the smart home network, identifying vulnerabilities, and recommending mitigation strategies to enhance security. The objectives were to evaluate the resilience of the network against potential cyber threats and provide actionable recommendations for strengthening its security measures. Findings from the penetration testing revealed several vulnerabilities within the network, including outdated firmware, default credentials, and insecure communication protocols. These vulnerabilities exposed the network to risks such as unauthorised access, data breaches, and malicious attacks. Recommendations to address these findings included regularly updating firmware/Software updates, installing patches, changing default credentials, implementing strong encryption protocols, and segmenting the network to isolate critical devices from potential threats.

Keywords -
LAN, smart home network, penetration testing, network setup, cyber security, vulnerabilities, cyber-attack.

I. NETWORKING AND NETWORK SETUPS

The process of sending and receiving data between nodes over a shared medium in an information system is known as networking [1] whereas it is also known as computer networking [1]. In addition to designing, building, and utilising a network, networking also includes managing, maintaining, and running the network's hardware, software, and policies [2]. A network consists of hardware components that form the network infrastructure, incorporating computers, hubs, switches, routers, and other devices. These are the components of the equipment that are crucial to the movement of data between locations via wires and radio waves, among other technologies that can link to one another via computer networking on a local area network (LAN) Alternatively, a more extensive network such as the internet or a private wide area network (WAN) can be utilised to exchange resources.
share services and communicate [3]. WANs typically span cities, nations, and even the entire planet and have a larger coverage area than LANs [4].

PROPOSED REALISTIC COMPLEX NETWORK SETUP

The proposed realistic complex network setup for the assessment is a LAN smart home network setup (see fig. 1). The network is a LAN (Local Area Network) smart home network designed to connect and control various smart home devices within a single residence. Its primary purpose is to provide automation, convenience, and security for homeowners by allowing them to monitor and manage smart home devices remotely.

To define the network setup, lengthy and thorough research was conducted on smart home network architectures, considering various types of devices commonly found in smart homes. The devices selected were chosen based on their wide availability and common utilisation in modern smart home setups.

This network setup is realistic and complex due to several factors:
1. Diverse Range of Devices in the network setup which includes a wide array of smart home devices such as routers, switches, IoT devices, security cameras, smart locks, and personal devices like smartphones and laptops.
2. Interconnectedness of the network setup, allowing for seamless communication and automation within the smart home environment.
3. Integration of IoT which adds complexity to the network, as they often have unique communication protocols and security requirements.
4. Security Considerations in the network setup such as implementing encryption protocols, updating firmware, and segmenting the network to isolate critical devices.

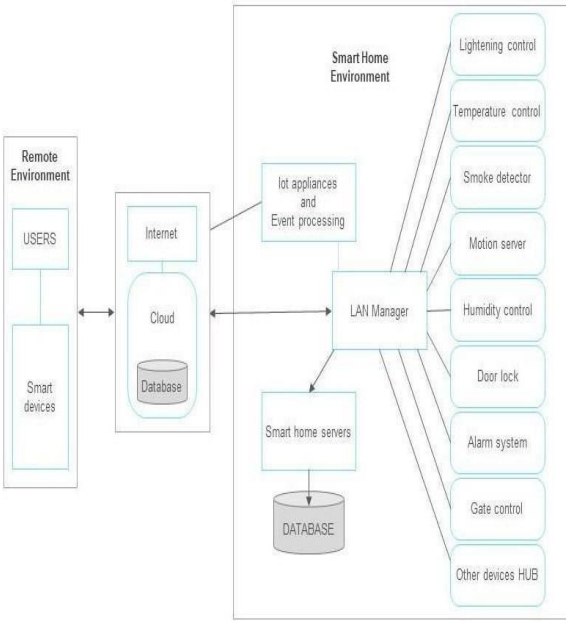

Figure 1: Network Setup Diagram of A Smart home Architecture

Figure 1 illustrates the network setup, depicting the main components and devices interconnected within the LAN smart home network. (See Table 1 for more information).

Device	**Model**	**Released Date**	**Brand**	**Specifications**
Router	TP-Link Tri-Band Wi-Fi 6 Mesh Router System (Deco BE85) [5]	May 2023	TP-Link	QoS, Access Point Mode, Tri-Band [5]
Network switch	SODOLA 48 Port 2.5GbE Switch [6]	Oct. 2023	Sodola	48 ports, Multi-Gig Smart Web Managed Switch [6]
Wi-Fi	TODA AIR AX1800 Mesh WiFi 6 Router [7]	August 2023	TODAAIR	Dual Band Wireless Internet Router [7]
Wireless controller / Hub	Homey Pro (Early 2023) [8]	July 2023	Homey	Compatible with Siri, Alexa & Google Home[8]
Virtual home Assistant/smart speaker	Amazon Echo Show 5 [9]	May 2023	Amazon	Smart display with 2x the bass and clearer sound + Alexa voice control [9]
Smart lock and doorbell	eufy Security Video Smart Lock E330 [10]	November 2023	eufySecurity	Door Lock, WiFi Door Lock,App Remote Control, 2K HD,Doorbell Camera [10]
Smart bulb	TP-Link Tapo Smart Light Bulbs [11]	Sept. 2023	TP-Link	Matter-Certified, 16M Colors RGBW LED Bulb, Dimmable, CRI>90, Voice Control w/Siri, Alexa &

				Google Assistant [11]
Smart Security cameras	Blink Outdoor 4 (4th Gen) [12]	August 2023	Blink	Smart security camera, two-way talk, HD live view, motion detection, set up in minutes, compatible with Alexa [12]
Air conditioning	Pro Breeze 10000 BTU [13]	May 2023	Pro Breeze	4 in 1, Smart Air Conditioner with Fan, Dehumidifier, Night, Timer, Window Venting Kit, Wifi Portable AC Unit [13]
Smart light switches	Eaton EWFD30-C2-BX-L[14]	May 2023	Eaton	120 Volts, Compatible with Alexa and Google Assistant [14]
Personal /home devices	iPhone 15 pro max [15]	Sept. 2023	Apple	iOS 17 [15]
	Microsoft surface pro laptop [16]	March 2023	Microsoft	Windows 11 Home [16]
	MacBook Air [17]	March 2024	Apple	Mac OS [17]

Table 1: Components of the LAN Smart Home Network [5-17]

JUSTIFICATION OF THE SMART HOME DEVICES IN NETWORK SETUP

The devices all listed in Table 1, selected for the smart home network setup were chosen based on several key considerations, including functionality, compatibility, reliability, and security. The selected router, TP-Link Tri-Band Wi-Fi 6 Mesh Router System (Deco BE85) offers offers WiFi 6 connectivity and mesh networking capabilities, ensuring reliable and high-speed internet access throughout the smart home network setup; SODOLA 48 Port 2.5GbE Switch provides Power over Ethernet (PoE) functionality, allowing for easy integration of PoE-enabled devices such as security cameras and access points; the smart home devices such as smart locks, bulbs, air-conditioning and cameras, were included to enable automation, enhance convenience, and improve security within the home. These devices offer functionalities such as remote monitoring, scheduling, and integration with voice assistants.

Additionally, all personal devices such as smartphones and laptops were carefully selected based on brand popularity and security features.

II. ATTACK VECTORS AND VULNERABILITIES

Attack vectors are the several techniques or routes that hackers take to obtain unauthorised access to a network, device, or computer system [18]. These attack vectors use vulnerabilities or flaws in the security measures of the system to perform harmful tasks. Attack vectors come in a variety of formats and can attack various parts of a system, such as network protocols, hardware, software, and end users [18]. Malware infections, phishing emails,

software exploits, brute force assaults, social engineering techniques, and network-based attacks like denial-of-service (DoS) or man-in-the-middle (MitM) attacks are a few examples of frequent attack vectors. In order to defend against cyber threats and keep systems and networks secure, it is crucial to comprehend and mitigate potential attack vectors [19, 20].

The selected smart home network setup comprises a variety of devices with different functionalities and vulnerabilities (see table 2). Therefore, it is crucial to consider attack vectors that can exploit these devices' weaknesses. Analysing these potential attack vectors, including recent real world incidents can help the smart home network's security posture.

Attack Vectors	**Type /Exploit**	**CVE number**	**Technique**	**Description**	**Date of incident**
Mercenary / spyware Infection	Software-based Vulnerability	CVE-2024-23296 [21]	Exploiting software vulnerabilities, Social engineering	Compromised Apple Devices may grant attackers Access to sensitive data, Smart Home Network devices like cameras, etc.	April 2024
Zero Day exploits	Smart Screen Vulnerability	CVE-2024-21412 [22]	Deceptive Websites click bait	Threat actors have the ability to breach system security, steal confidential information, and exfiltrate sensitive data.	Feb. 2024
Windows Kerberos Machine-in-the-middle (MITM)	Security Feature Bypass Vulnerability	CVE-2024-20674 [23]	Sending a malicious Kerberos message to a client machine	Attackers attempt to crack passwords to gain unauthorized access	Jan. 2024 [23]

Table 2: Recent Real word Malware Attacks on Smart Home Network Devices [21-23]

Apple Mercenary/ Spyware Attack (CVE-2024-23296):

The Apple Mercenary/Spyware Attack targets devices running iOS, including iPhones and iPads, with the aim of infiltrating these devices to surveil users and steal sensitive information. Attackers may be motivated by espionage, identity theft, or financial gain [21]. This attack vector exploits a zero-day vulnerability (CVE-2024-23296) in the iOS kernel and RTKit component, allowing attackers to execute arbitrary code with kernel privileges. The attack may involve malicious apps or crafted web content that triggers the exploit when accessed or opened on the victim's device [24]. The primary targets of this attack are Apple devices running iOS, including iPhone and iPad models. These devices are widely used and store a wealth of personal and sensitive information including smart home device passwords making them lucrative targets for attackers looking to break into homes.

Windows SmartScreen Vulnerability (CVE-2024-21412):

The SmartScreen Vulnerability targets Microsoft Defender SmartScreen, a feature designed to protect users from malicious websites and downloads [22]. The CVE-2024-21412 vulnerability was discovered in February 2024 when attackers exploited this vulnerability to bypass SmartScreen protections and deliver malware and phishing content to unsuspecting users. This attack vector exploits a zero-day vulnerability (CVE-2024-21412) in Microsoft Defender SmartScreen, allowing attackers to circumvent the protection mechanisms and trick the system into classifying malicious content as safe. This may involve exploiting flaws in the way SmartScreen analyses URLs, files, or digital signatures to evade detection and deliver harmful payloads to victims' devices.

The SmartScreen Vulnerability primarily affects devices running Microsoft Windows operating systems with Microsoft Defender enabled. This includes desktops, laptops, and servers using Windows 10, Windows 11, or Windows Server operating systems [25].

Windows Kerberos Machine-in-the-middle (MITM)CVE-2024-20674:

The Windows Kerberos Machine-in-the-Middle (MITM) Vulnerability targets the Kerberos authentication protocol used in Microsoft Windows environments [26]. Attackers exploit this vulnerability to intercept and manipulate network traffic, impersonate legitimate users or services, and gain unauthorised access to sensitive information or resources within the network. This attack vector exploits a flaw in the Kerberos protocol implementation on Windows systems, allowing attackers to intercept and manipulate authentication requests and responses between clients and servers. By positioning themselves as a "middleman" between the client and server, attackers can capture authentication credentials, forge tickets, or impersonate legitimate users to gain unauthorized access to network resources [26].

The Windows Kerberos MITM Vulnerability affects devices running Microsoft Windows operating systems that utilise the Kerberos authentication protocol for network authentication. This includes domain controllers, servers, workstations, and other Windows-based devices within the network.

The CVE-2024-20674 vulnerability was discovered in January 2024 when Microsoft issued a security patch to address this vulnerability promptly after its discovery to mitigate the risk to users' devices and network environments.

III. MITIGATION SOLUTIONS

To effectively mitigate the vulnerabilities outlined, a comprehensive approach encompassing technical measures, user education, and proactive security practices is necessary.

Regular Software Updates on Smart Devices:

Implementation of a strict home security policy to make sure that all software, like operating systems, apps, and firmware, gets the latest security patches and fixes provided by the respective vendors can serve as a vital component of a strong cyber security system [27].

Network Segmentation:

For large homes with complete smart home automation, it is advisable to segment the network into separate zones based on the function and sensitivity of data to limit the spread of cyber-attacks and contain potential breaches [28]. Additionally, to regulate between segments, implement firewalls and access points for security purposes.

Enable Strong Multifactor Authentication Mechanisms:

Enforcing the use of powerful authentication techniques, such as multi-factor authentication (MFA), is essential for securely accessing vital systems and confidential information., this decision would prevent unauthorised access even if password credentials are compromised [29].

Endpoint Protection and Encryption:

Implement endpoint protection solutions, such as antivirus software, intrusion detection systems (IDS), and endpoint detection and response (EDR) tools, to identify and prevent dangerous activities on devices connected to the network [27].

Also, buying only smart devices from trusted brands that encrypt sensitive data using strong encryption algorithms, will prevent unauthorised access in case of data interception or theft.

Third-Party Risk Management:

It is also important to conduct regular security assessments and due diligence of third-party vendors, suppliers, and service providers of smart devices and updates to ensure they adhere to security best practices and standards [27].

Overall, addressing vulnerabilities such as SmartScreen Vulnerability, Apple Mercenary/Spyware Attack, and Windows Kerberos MITM Vulnerability requires a multi-faceted approach that includes regular software updates and the implementation of security best practices. By implementing these comprehensive mitigation solutions, smart homeowners can strengthen their security posture, mitigate potential vulnerabilities, and effectively defend against a wide range of cyber threats in today's dynamic threat evolution.

IV. CONCLUSION

With the modern-day popularity of smart homes, it is imperative that safeguarding smart home networks against evolving cyber threats undertake a multifaceted approach that encompasses proactive measures, vigilant monitoring, and continuous adaptation to emerging risks. Through the assessment of potential attack vectors and the implementation of comprehensive mitigation solutions, homeowners can enhance the security posture of their smart home environments and mitigate the risks associated with malicious exploitation.

The assessment revealed a myriad of attack vectors targeting various components of the smart home network, including vulnerabilities in popular devices and software applications. From Apple Mercenary/ Spyware Attack (CVE-2024-23296) to SmartScreen Vulnerability (CVE-2024-21412) and Windows Kerberos Machine-in-the-middle (MITM) (CVE-2024-20674), each presents unique challenges and potential risks to the integrity, confidentiality, and availability of smart home systems. However, by adopting mitigation strategies such as regular software updates, network segmentation, Endpoint protection and third-party risk management, homeowners can significantly reduce their exposure to cyber threats and enhance the resilience of their smart home networks.

In conclusion, this assessment highlights the importance of securing smart home networks against cyber threats to safeguard the privacy and security of residents. By addressing identified vulnerabilities and implementing recommended mitigation measures, homeowners can enhance the resilience of their smart home network and mitigate the risk of potential cyber attacks.

V. REFERENCES

[1] P. Kirvan and J. Scarpati, “Networking (computer),” 2024. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/networking [Accessed on: Apr. 30, 2024].

[2] T. Ruha, “Cybersecurity of Computer Networks,” Thesis, 2018. [Online]. Available: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://core.ac.uk/download/pdf/161424802.pdf&ved=2ahUKEwjZodfw1OuFAxXRQkEAHTCrB48QFnoECB4QAQ&usg=AOvVaw1YIJLIF8n19Zw9kNvWVZOp [Accessed on: Apr. 30, 2024].

[3] B. Afroj and S. Vijay, “Cybersecurity in Networking Devices,” 2021. [Online]. Available: https://www.researchgate.net/publication/355875716_Cybersecurity_in_Networking_Devices/citation/download [Accessed on: Apr. 30, 2024].

[4] A. Saravanan, “Introduction to Networking,” 2012. [Online] Available: https://www.researchgate.net/publication/323511648_INTRODUCTION_TO_NETWORKING/citation/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 [Accessed on: Apr. 29, 2024].

[5] Amazon, “TP-Link Tri-Band WiFi 7 BE22000,” 2013. [Online]. Available: https://www.amazon.com/TP-Link-Deco-BE85-AI-Roaming-HomeShield/dp/B0C4W31L4N?tag=w050b-20&asc_source=&asc_campaign=615b126d272def4b666617ae&asc_refurl=https%3A%2F%2Fwww.wired.com%2Fstory%2Fbest-mesh-wifi-routers&ascsubtag=615b126d272def4b666617ae[Accessed on: Apr. 29, 2024].

[6] Amazon, “SODOLA 48 Port 2.5GbE Switch,” 2024. [Online]. Available: https://www.amazon.com/Managed-Sports-Mega-Switch-QSFP-Multi-Gig/dp/B0CKT3KF8W [Accessed on: Apr. 29, 2024].

[7] Amazon, “TODAAIR AX1800 Mesh WiFi 6 Router,” 2024. [Online]. Available: https://www.amazon.com/TODAAIR-Wireless-Internet-Connect-Coverage/dp/B0CP7GDYRS/ref=mp_s_a_1_7_sspa?crid=8MFCMBSWXJL&dib=eyJ2IjoiMSJ9.RvsvirkM3ruJgsu4SzS7LDfoZjYrLCHFMh2yGTX5TUczOvjfNRgw5VCuVprkYOj3S2CCdvqMczx9QQtDTs5GZhqrCdJHPyg7UI2Y-ScD4PjjDHigLQLVuLFGLI1_KQFrmCaly_YQhb41vGl-IhJjrgB9FPOLysjDB1S2oQ9zTJCUUqPwVg51CQ

_0N0l1WwdkoQCCgFkznBWLUdRrIbpFVw.S40TK25MEEehqYWuna9CCD4u8jhhy6ZEPix1KRk3T1M&dib_tag=se&keywords=best+wifi+router+for+large+home+released+in+2023&qid=1714549420&sprefix=best+wifi+router+for+large+home+released+in+2023%2Caps%2C603&sr=8-7-spons&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9zZWFyY2hfbXRm&psc=1 [Accessed on: Apr. 29, 2024].

[8] Amazon, "Homey Pro (Early 2023)," 2023. [Online]. Available: https://www.amazon.com/Homey-Early-2023-Smart-Automation/dp/B0C5RFQNN4/ref=mp_s_a_1_1?adgrpid=160760734931&dib=eyJ2IjoiMSJ9.F25JKkDBNX3En84YeQvhY2k5IXm9I_64UhRcMwNEiogi-g7_AYVnKOZuNPhg1ACQWfayEFjbhaSzSSrB6K-qXBEu3u01gcOdshraNBHZyGHbkyyLfUem3na0j-fPdY5NLp7JxL3y9VLji9-qJwgs8Do7XDHwY0KTYt9Fpwbv6gkRahKsev9Fs6l9itN9xxwA.R3Y4qq8lt17k9eF5KuFV3p7x5DEyGYzc1dqp_Xj_OPI&dib_tag=se&gad_source=1&hvadid=678748497111&hvdev=m&hvlocphy=1010296&hvnetw=g&hvqmt=b&hvrand=9250200421512713443&hvtargid=kwd-887643651836&hydadcr=22264_13517319&keywords=homey+pro+hub&qid=1714548428&sr=8-1 [Accessed on: Apr. 29, 2024].

[9] Amazon, "Echo Show 5 (3rd Gen," 2023. [Online]. Available: https://www.amazon.com/All-new-release-display-clearer-Glacier/dp/B09B2QTGFY/ref=mp_s_a_1_2?crid=2QS5MSBEE454Z&dib=eyJ2IjoiMSJ9.XqlFzPVFTQEgAMEkBgl0aMfknWtTodcjohhsIiZ-mJfxOQiKjH3gsEEubDL6MTdhYGF7DScKl98-1r2zbyqz38iFH5lEgoHj_FK4AOVWdLBNq41IP8YrwlA9TaZrD6TT-L38uDwof0twViC0hd3ui9faJL_R330uIuNJ_qLDJYceBzAL9hXAbZECFssNPagK9Nusqy_q8ua08gMDz7wfVA.pSsl8T3hQ-H0zlR4LkehM-mkKJZETl_azaZxsQtcIvQ&dib_tag=se&keywords=echo+4+gen+2023&qid=1714549841&sprefix=echo+4+gen%2Caps%2C2376&sr=8-2 [Accessed on: Apr. 29, 2024].

[10] Amazon, "eufy Security Video Smart Lock E330," 2023. [Online]. Available: https://www.amazon.com/eufy-Security-Doorbell-Fingerprint-Keyless/dp/B0CJXVK5S6 [Accessed on: Apr. 29, 2024].

[11] Amazon, "TP-Link Tapo Smart Light Bulbs,," 2023. [Online]. Available: https://www.amazon.com/Tapo-Brightness-Equivalent-Matter-Certified-L535E/dp/B0CFG9MXKD/ref=mp_s_a_1_3?adgrpid=152355033062&dib=eyJ2IjoiMSJ9.C0Mp2PIn6VG7VLca8Xll5uaDHuvSCZq_kC9yBEDUj51lQpNut42jYs9Z68xcxtKzotPF5MOrPcIM-c1q8_zqqVQEHha_JT76lincLs4ElSTVc_NAdLy0hanF09Jbis9v9s5HUtqRmSwh70qnFc4Kru4R8BFdYLsTy8j7bVpj4NEKdGRKMmgzw1ZsDghMgCqkbxd4nvU-kkneKq3xKwXuqA.MTmxkn9xDqTDnibj0UqbtCAPSnRJesM5BG0S7ulTzV4&dib_tag=se&hvadid=678839917391&hvdev=m&hvlocphy=21572&hvnetw=g&hvqmt=b&hvrand=14500999330930547977&hvtargid=kwd-1572208965998&hydadcr=15228_13706215&keywords=matter+smart+bulb&qid=1714552091&sr=8-3 [Accessed on: Apr. 29, 2024].

[12] Amazon, "Blink Outdoor 4 (4th Gen)," 2023. [Online]. Available: https://www.amazon.com/Blink-Outdoor-4th-Gen-Mini/dp/B0BWFFQZ7G/ref=mp_s_a_1_5_ffob_sspa?adgrpid=79683220977&dib=eyJ2IjoiMSJ9.k_-TqStjncUDWwt7lRxXOYioGzaRpTpQHyddxHGiyxHoAUQe9p-ZPS8w69eGnMmbrgtkm_Eu1RI5fyiE58VjAvZIH727SaCygxJVp0ErrSgBfeNTFNHH8COMr8ZJsrONxOC01i3YgwtbopsoSaecHeOm3aU7qxP6orPyhk17CHXhJZA7zbtDwRUOyEGoy-nHXoGgt5LlPjedVjyE75YCQA.kJ-SQxOzpdjBMtg1bEVkGRgX3cuuSrpGLVPo-Ef_z2c&dib_tag=se&hvadid=585412350214&hvdev=m&hvlocphy=21572&hvnetw=g&hvqmt=b&hvrand=7184363155386600614&hvtargid=kwd-319680930714&hydadcr=25091_13496241&keywords=smart+home+security+camera&qid=1714552509&sr=8-5-spons&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9zZWFyY2hfbXRm&psc=1 [Accessed on: Apr. 29, 2024].

[13] Amazon, "Pro Breeze 4 in 1 Portable Air Conditioner," 2023. [Online]. Available: https://www.amazon.com/dp/B08Q7JVZ6B/ref=sspa_mw_detail_0?ie=UTF8&psc=1&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9kZXRhaWwp13NParams [Accessed on: Apr. 29, 2024].

[14] Amazon, "Eaton EWFD30-C2-BX-L Wi-Fi Smart Universal Dimmer," 2023. [Online]. Available: https://www.amazon.com/Eaton-EWFD30-C2-BX-L-Universal-Compatible-

Assistant/dp/B0B1H1KPX6/ref=mp_s_a_1_1_sspa?dib=eyJ2IjoiMSJ9.MZeGpYpq4NNpMO9W5SmFvKCZq040jmqBtF2q6mDpOHWvp_uy4P1UlG_AvIGqRJWq-fdafAd3HdVTm3YQgQAi6ma8HfNK1tIRHMFpQ_-Wo8o85RThr7VfbnO1p7lOLmEzzqtWlZggo5cbmm67cxQEvDSyUeNxD8bzZWSgIpijc298_Pq-iWSMZS540lVPjvPO8H2vPwhfQJ-0HJg3KPJ1xQ.CYKWC5Np6H--x6fFsFEEuJ7DUIYgGoCKA6EbvfNg8BI&dib_tag=se&keywords=smart+light+switches+2023+works+with+Alexa&qid=1714554508&sr=8-1-spons&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9zZWFyY2hfYXRm&psc=1 [Accessed on: Apr. 28, 2024].

[15] Apple, “iPhone 15 Pro,” 2023. [Online]. Available: https://www.apple.com/ng/iphone-15-pro/specs/ [Accessed on: Apr. 29, 2024].

[16] Amazon, “Microsoft QIL-00035 Surface Pro 9 13,” 2023. [Online]. Available: https://www.amazon.com/Microsoft-QIL-00035-Signature-Mechanical-Protection/dp/B0BK2DDPDT/ref=mp_s_a_1_1_sspa?adgrpid=155964676459&dib=eyJ2IjoiMSJ9.xfrKHuEVVbXTPCvdNUk4DkpEQpBD5yjQajzpXK_KjmlAgR94r2Hap3ufzRBlSzbYraLC5_FLQwE4TKyYNXO8lKC0Uum4-yL-pImDKeCvoyJHGOKhdEmuOl3204nX-T9ZzPJiBNyLzavnKKOPT37_J5kyHRipOtG02cKuNrpdIBeWxddKPKqFPXzixu8OFzi-lhYZOIWDKljQD2pMQmLF_A.WyY72LIpuA1Bq8_88XQJyZo_TrJZMY4ol00MoebeKiE&dib_tag=se&gad_source=1&hvadid=681380681503&hvdev=m&hvlocphy=21572&hvnetw=g&hvqmt=b&hvrand=6218233022638660987&hvtargid=kwd-837589122647&hydadcr=12603_13401784&keywords=surface+pro+2023&qid=1714554894&sr=8-1-spons&sp_csd=d2lkZ2V0TmFtZT1zcF9waG9uZV9zZWFyY2hfYXRm&psc=1 [Accessed on: Apr. 29, 2024].

[17] Amazon, “Apple 2024 MacBook Air ,” 2024. [Online]. Available: https://www.amazon.com/Apple-2024-MacBook-13-inch-Laptop/dp/B0CX22ZW1T?asc_source=verso&asc_campaign=5a78e59756f21920c2bf083b&asc_refurl=https%3A%2F%2Fwww.wired.com%2Fstory%2Fwhich-macbook-should-you-buy&ascsubtag=5a78e59756f21920c2bf083b&tag=w050b-20 [Accessed on: Apr. 29, 2024].

[18] Cloudflare, “What is an attack vector?,” 2023. [Online]. Available: https://www.cloudflare.com/learning/security/glossary/attack-vector/ [Accessed on: Apr. 29, 2024].

[19] K. Fidler, “Smart speakers pose threat to particular group of people,” 2024. [Online]. Available: https://www.google.com/amp/s/metro.co.uk/2024/03/29/experts-share-safety-warning-smart-speakers-homes-20552221/amp/ [Accessed on: Apr. 29, 2024].

[20]S. Kemp et al., “The digital harms of smart home devices: A systematic literature review,” *Computers in Human Behavior*, Vol.145,, pp. 107-770, Aug. 2023.

[21] A. Spadafora, “Apple just fixed two major iPhone security flaws — install these emergency updates now,” 2024. [Online]. Available: https://www.tomsguide.com/phones/iphones/apple-just-fixed-two-major-iphone-security-flaws-install-these-emergency-updates-now [Accessed on: Apr. 29, 2024].

[22] Trend Micro, “SmartScreen Vulnerability: CVE-2024-21412 Facts and Fixes,” 2024. [Online]. Available: https://www.trendmicro.com/en_us/research/24/b/cve-2024-21412-facts-and-fixes.html [Accessed on: Apr. 29, 2024].

[23] Tenable, “CVE-2024-20674 | Windows Kerberos Security Feature Bypass Vulnerability,” 2024. [Online]. Available: https://www.tenable.com/blog/microsofts-january-2024-patch-tuesday-addresses-48-cves-cve-2024-20674#:~:text=CVE%2D2024%2D20674%20is%20a,to%20the%20Microsoft%20Exploitability%20Index [Accessed on: Apr. 29, 2024].

[24] Reuters, “Apple drops term 'state-sponsored' attacks from its threat notification policy,” 2024. [Online]. Available: https://www.reuters.com/technology/cybersecurity/apple-warns-users-mercenary-spyware-attack-91-countries-including-india-et-2024-04-11/ [Accessed on: Apr. 29, 2024].

[25] Microsoft, “CVE-2024-21412,” 2024. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412 [Accessed on: Apr. 29, 2024].

[26] Z. Zorz, “Microsoft fixes critical flaws in Windows Kerberos, Hyper-V (CVE-2024-20674, CVE-2024-20700),” 2024. [Online]. Available:]https://www.helpnetsecurity.com/2024/01/09/cve-

2024-20674-cve-2024-20700/ [Accessed on: Apr. 29, 2024].
[27] T. Lacomer, “Is Smart Home Security Easily Hacked? Here's Everything You Should Know,” 2024. [online]. Available: https://www.cnet.com/home/security/is-smart-home-security-easily-hacked-in-2024-heres-everything-you-should-know/ [Accessed on: Apr. 29, 2024].
[28] J. Cohen and S. Mlot, “Stay Safe: 8 Ways to Protect Your Smart Home From Hackers,” 2023. [Online]. Available: https://www.pcmag.com/how-to/protect-your-smart-home-from-hackers [Accessed on: Apr. 29, 2024].